Exchange 2000 QuickDoc

The Ultimate Guide to....Permissions

QD202 **Version 2.2**

Compiled by:

Paul Bowden, Program Manager
Microsoft Exchange Server Product Unit

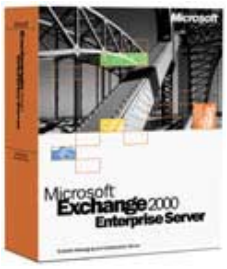
© 2000 Microsoft Corporation. All rights reserved.

The information contained in this White Paper represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

BackOffice logo, Microsoft, Win32, Windows, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other product or company names mentioned herein may be the trademarks of their respective owners.

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA



Introduction to Permissions

This document describes the minimum permissions required for installation and management of Exchange 2000.

Please note that you may not need to explicitly set the role outlined in this document to perform the desired action, as roles can be supersets. For example:

Administrative Group level:

'Exchange Administrator' incorporates 'Exchange View Only Administrator'.

'Exchange Full Administrator' incorporates 'Exchange Administrator' and 'Exchange View Only Administrator'.

Organization level:

'Exchange View Only Administrator' incorporates 'Exchange View Only Administrator' at the Administrative Group level

'Exchange Administrator' incorporates 'Exchange View Only Administrator' at the Organization level and 'Exchange Administrator' and 'Exchange View Only Administrator' at the Administrative Group level

'Exchange Full Administrator' incorporates all other permissions at both the Organization and Administrative Group levels

Graphical representation of permissions:

Granted Permissions (below) vs. Effective Permissions (right)	AG: View	AG: Admin	AG: Full Admin	ORG: View	ORG: Admin	ORG: Full Admin
AG: Exchange View Only Administrator	Yes*					
AG: Exchange Administrator	Yes*	Yes*				
AG: Exchange Full Administrator	Yes*	Yes*	Yes*			
ORG: Exchange View Only Administrator	Yes			Yes		
ORG: Exchange Administrator	Yes	Yes		Yes	Yes	
ORG: Exchange Full Administrator	Yes	Yes	Yes	Yes	Yes	Yes

* = Local Administrative Group only

Active Directory Connector

What permissions do I need to install the first Active Directory Connector (ADC) in my Windows 2000 Active Directory forest?

The installation of the first ADC involves updating the schema of the Active Directory as well as copying the binaries across to the local machine. Therefore, you will need to be logged on as a user with the following Active Directory permissions:

Schema Admins

Enterprise Admins

Member of the local Administrators group on the target machine

Alternatively, a Schema Administrator can use the /SchemaOnly switch with the ADC setup program to make the additions to the Active Directory. In this scenario, the person who actually installs the ADC service does not need to be a member of the Schema Admins group.

What permissions do I need to install subsequent Active Directory Connectors into my Active Directory forest?

As the schema should already be updated, you will need the following Active Directory permissions:

Enterprise Admins

Member of the local Administrators group on the target machine

When installing the Active Directory Connector, I need to enter a service account. Why is this required when Exchange 2000 services start up as "LocalSystem"? What permissions will the service account require?

The ADC requires a service account because a subset of the ADC technology is shipped with Windows 2000. Exchange 2000 has features to prepare the AD forest and domains for installation of the server (/ForestPrep and /DomainPrep). Part of this preparation involves the setting of permissions for LocalSystem services to the Active Directory. As the ADC can be used without Exchange 2000 being installed, a separate service account is used to achieve the same functionality.

The ADC service account requires the following permissions:

Member of the Builtin\Administrators group

Member of Enterprise Admins if used solely with Windows 2000

Member of Enterprise Admins OR 'Exchange Full Administrator' role if used with Exchange 2000

When I create a Connection Agreement in the Active Directory Connector, I need to specify the credentials for accessing the Active Directory and Exchange Directory. What permissions does this account need?

Exchange 5.5:

'Admin' role to the Exchange 5.5 Site naming context

'Admin' role to the Exchange 5.5 Organization naming context

Active Directory:

Domain Admins (local)

'Exchange View Only Administrator' role to the Exchange 2000 Organization

Exchange 2000

What permissions do I need to run the /ForestPrep switch for Exchange 2000 SETUP?

ForestPrep will update the Active Directory schema and create the Exchange Organization object. Additionally, you will be given the opportunity to specify the first Exchange 2000 Administrator (this can be a user or group object). You will need to be logged on to the Active Directory as a user with the following permissions:

Schema Admins

Enterprise Admins

ForestPrep must be run in the domain that contains the Active Directory Schema Master. By default, this will be the root domain in the forest.

If I choose to join an existing Exchange 5.5 Organization during ForestPrep, what permissions do I need to the Exchange 5.5 Organization?

'Admin' role to the Exchange 5.5 Site naming context (for the site that you're joining)

'Admin role to the Exchange 5.5 Configuration naming context (for the site that you're joining)

Additionally, you will need to know the service account name and password for the site that relates to the server that you specify. If the 5.5 service account is not in a domain that is not part of the AD forest, then you will need to create a one-way trust from the forest root domain to the domain that contains the 5.5 service account.

What permissions do I need to run the /DomainPrep switch for Exchange 2000 SETUP?

DomainPrep will create a new "Exchange Domain Servers" Global Group, a "Exchange Enterprise Servers" Local Group, and seed the permissions so that Exchange server can access the Active Directory. To run DomainPrep, you should be logged on as a user with the following permissions:

Domain Admins (of the local domain)

What function do the 'Exchange Domain Servers' and 'Exchange Enterprise Servers' groups perform?

Both of these groups are created through DomainPrep. They reside in the 'Users' container in the domain and must not be moved or renamed. Each time a computer is installed with Exchange 2000, its computer account is added to the local 'Exchange Domain Servers' global security group. In turn, this group is a member of the 'Exchange Enterprise Servers' local security group in each domain. The Recipient Update Service (RUS) is responsible for ensuring that all Exchange group nestings are complete within the forest. The 'Exchange Enterprise Servers' group is given various permissions on the domain naming context. Through these inherited permissions, the RUS is able to modify Exchange specific attributes on domain accounts.

What permissions do I need to install my first Exchange 2000 server?

You will need to be logged on with the following permissions:

'Exchange Full Administrator' role (defined during ForestPrep)

Member of the local Administrators group on the target machine

Additionally, if you are joining an existing Exchange 5.5 Site, your account must have the following permissions to the Exchange 5.5 directory, and the installer must know the Site Services Account name and password:

'Admin' role on the Site naming context

'Admin' role on the Configuration naming context

How do I delegate permissions to other users so that they can manage Exchange 2000?

Use the 'Exchange Administration Delegation Wizard'. You can find this in the Exchange System Manager by right-clicking on either the Organization or Administrative Group objects.

You will need to be logged on as a user with the 'Exchange Full Administrator' role to the Organization to use the Exchange delegation wizard.

If I move the Exchange 2000 computer accounts to a different OU in the Active Directory, will this effect my Exchange permissions and delegation?

No.

What's the difference between the 'Exchange Full Administrator' and the 'Exchange Administrator' roles?

An 'Exchange Full Administrator' is able to manipulate any Exchange object in the configuration naming context. Additionally, full administrators have permissions to modify the "Security" tab on the following objects:

- Exchange Databases
- MAPI and Application Folder hierarchies
- Address Lists

An 'Exchange Administrator' can manipulate any Exchange object, but will not have the ability of delegating permissions or changing the "Security" tab on the Exchange objects listed above.

If I grant a user/group permissions at the Exchange Organization level, do these automatically flow down to all Administrative Groups?

Yes.

What permissions do I need to install subsequent Exchange 2000 servers?

You will need to be logged on with the following permissions:

'Exchange Full Administrator' (as defined during ForestPrep) OR a delegated 'Exchange Full Administrator' at the Organization level

Member of the local Administrators group on the target machine

What permissions do I need to install Exchange 2000 in a cluster configuration?

You should install the server software and create the System Attendant resource by logging on as the cluster service account. This account will also need the following permissions:

'Exchange Full Administrator' (as defined during ForestPrep) OR a delegated 'Exchange Full Administrator' at the Organization level

Member of the local Administrators group on both nodes

What permissions do I need to upgrade an Exchange 5.5 server to Exchange 2000?

First of all, the Exchange 5.5 server must be running on Windows 2000 in an Active Directory domain. You will need to be logged on as a user who has the following permissions:

Exchange 5.5:

'Admin' role to the Exchange Organization naming context

'Admin' role to the Exchange Site naming context

'Admin' role to the Exchange Configuration naming context

Active Directory:

'Exchange Full Administrator' (as defined during ForestPrep) OR a delegated 'Exchange Full Administrator' at the Organization level

Member of the local Administrators group on the target machine

I have a third-party messaging application that requires full access to each users mailbox. With Exchange 5.5 we grant a special account Service Account Admin permissions and then tell the application to use this account. How can I achieve similar functionality in Exchange 2000?

Exchange 2000 security works very differently to Exchange 5.5. In fact, Exchange 2000 does not use a site service account, instead, all services start up as the local computer account.

There are a few different ways to get the desired effect. One of the easiest is to make your special application account a member of the "Exchange Domain Servers" groups (in any domain). This account will now have the same permissions as Exchange 2000. However, be warned that the account that you have added can really do anything it likes to the Exchange data.

Why did we have a special service account in Exchange 5.5, when Exchange 2000 services can start up as the Local System or built-in computer account?

Exchange 5.5 required a special logon account for it's services due to a limitation with Windows NT4.0. Although local computer accounts in NT4.0 had tokens, they did not have credentials, therefore, one computer account could not authenticate to another. We use Kerberos authentication in Windows 2000, and computer accounts have both tokens and credentials.

Using the local computer account is more secure than an administrator specified account, for the following reasons:

- Local computer password is random hex rather than a human-readable string
- Local computer password changes automatically every thirty days
- The Exchange 5.5 service account had to be excluded from lockout policies as a brute force attempt to logon could disable the account and shut down the Exchange services

The computer account for my Exchange 2000 server was accidentally deleted from the Active Directory. Although I can re-create it, will the Exchange 2000 services work correctly?

If you simply re-add the computer account, the Exchange services will start, although you may encounter some issues. The computer account is assigned various permissions in the Active Directory during the Exchange 2000 SETUP process. Therefore, by re-running SETUP and choosing the "Reinstall" option, these permissions will be granted for your new computer account.

You should also check the local "Exchange Domain Servers" group within the domain to ensure that your new computer account is a member. The System Attendant will attempt to add the computer account to this group upon start-up, however if this process is unsuccessful, you will need to add the account manually.

Exchange 2000 Management

What permissions do I need to be able to create and delete mailboxes?

First, you need to have permissions to create a user object in the Active Directory. For example, you could be a Domain Admin, or you may have delegated access to a specific Organization Unit. Then you need the following Exchange permissions:

> *'Exchange View Only Administrator' role to the Administrative Group where the target Exchange 2000 server exists*

Additionally, if you manage Public Folder objects, you should ensure that your administration account (i.e. the account that you are logged on as when you manipulate objects in the Exchange System Manager) is mail/mailbox-enabled.

What permissions do I need to be able to move a mailbox from Exchange 5.5 to Exchange 2000 in the same Site/Administrative Group?

When you invoke the move from the Active Directory Users and Computers snap-in, the mailbox is transferred between the two servers, and then the current credentials are used to update the Home-MTA and Home-MDB attributes on the user/mailbox object.

You will need the following permissions:

Exchange 5.5:

> *'Admin' to the Site naming context*

Active Directory:

> *Member of Domain Admins OR Account Operators group to the local domain*
>
> *'Exchange Administrator' role to the Administration Group*

What permissions do I need to be able to configure Routing Groups and Connectors?

In this scenario, you are not directly affecting user account objects, therefore you only need the following permissions:

> *'Exchange Administrator' role to the Administrative Group where the target Routing Group exists*

Note: Routing Group Connectors (RGC) are uni-directional. To create a bi-directional RGC to a Routing Group which lies outside of the local Administrative Group, you will also need to have Admin permissions to the remote Administrative Group.

If you need to define the global message formats for specific outbound domains or need to specify global message thresholds, you will need the following permissions:

> *'Exchange Administrator' role to the Exchange Organization*

If you will also manage the SMTP service, your account will need to be a member of the built-in Administrators group on each Exchange server (for metabase access).

What permissions do I need to be able to manipulate message queues?

To view the message queues in the Exchange System Manager, you will need the following permissions:

> *'Exchange View Only Administrator' role on the Administrative Group where the connector exists*
>
> *Member of the local Administrators group on the target machine*

To remove messages from queues, you will need the following permissions:

'Exchange Administrator' role on the Administrative Group where the connector exists

Member of the local Administrators group on the target machine

What permissions do I need to manage Instant Messaging?

To create and manage an Instant Messaging virtual server, you need the following permissions:

'Exchange Administrator' role to the Administrative Group where the IM server will be created

If you need to change the firewall topology information for Instant Messaging within your organization, you will need these additional permissions:

'Exchange Administrator' role to the Exchange Organization

To enable a user for Instant Messaging you need permissions in the domain naming context of the Active Directory domain. Enabling a user for IM involves changing some attributes on the user account, therefore you will need to have permissions on the organization unit where the user exists. For most companies, the administrator who creates/deletes user accounts and mailboxes will also be responsible for enabling the user for Instant Messaging.

What permissions do I need to install Exchange Conferencing server?

You will need to be logged on as a user with the 'Exchange Full Administrator' role at the Exchange 2000 Organization level.

How do the Exchange Administrator roles effect Exchange Conferencing management?

Exchange Full Administrator role at the Administrative Group level

This role CAN:

- Install & remove Conferencing services
- Stop and Start Conferencing services
- Create/Delete the Conference Calendar mailbox and resource mailboxes
- Add/Remove/Configure Conferencing Technology Providers (CTPs)
- View/Modify Conference Settings.

Exchange Administrator role at the Administrative Group level

This role CAN:

- Create/Delete the Conference Calendar mailbox and resource mailboxes
- Add/Remove/Configure Conferencing Technology Providers (CTPs)
- View/Modify Conference Settings

This role CANNOT:

- Install & remove Conferencing services
- Stop and Start Conferencing Services (unless local Administrator permissions are granted)

Exchange View Only Administrator role at the Administrative Group level

This role CAN:

- View Conference Settings

This role CANNOT:

- Install & remove Conferencing services
- Stop and Start Conferencing Services (unless local Administrator permissions are granted)`
- Create/Delete the Conference Calendar mailbox and resource mailboxes
- Add/Remove/Configure Conferencing Technology Providers (CTPs)
- Modify Conference Settings

What permissions do I need to create a new Administrative Group?

You will need to be logged on as a user with the following permissions:

'Exchange Administrator' role to the Exchange Organization

With Exchange Server 5.5 and Windows NT4.0 I had two support teams, one for the Exchange Directory and one for the SAM. Although I can see the benefits of unified administration with Exchange 2000 and Active Directory, can I still split out the user creation and mailbox creation roles?

You can achieve this scenario by restricting permissions to the Exchange attributes using the Windows 2000 Delegation Wizard. Simply set the delegated user or group to have read/write access to the 'private-information' and 'public-information' property sets.

Appendix A: Permissions granted during SETUP

PERMISSIONS ON OBJECTS IN THE EXCHANGE CONFIGURATION TREE:

Microsoft Exchange container

Cn=Microsoft Exchange,cn=Services,cn=Configuration,dc=<domain>					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During ForestPrep phase					
Authenticated Users	✔			ACTRL_DS_LIST | ACTRL_DS_READ_PROP	
Designated admin account	✔		✔	DS_AM_FULL_CONTROL	
During server install					
Exchange Domain Servers	✔		✔	STANDARD_RIGHTS_READ | ACTRL_DS_READ_PROP | ACTRL_DS_LIST	
During ADC setup					
Exchange Services	✔		✔	DS_AM_FULL_CONTROL	

ADC Connection Agreement container

cn=Active Directory Connections,cn=Microsoft Exchange,cn=Services,cn=Configuration,dc=<domain>					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During server install					
Exchange Domain Servers	✔		✔	DS_AM_FULL_CONTROL	

Organization container

cn=<organization>,cn=Microsoft Exchange,cn=Services,cn=Configuration,dc=<domain>					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property/ Applies To**
During ForestPrep phase					
Authenticated Users	✔			ACTRL_DS_LIST_OBJECT | ACTRL_DS_READ_PROP	
Designated admin account		✔	✔	Send-As	
Designated admin account		✔	✔	Receive-As	
During Server install					
“Enterprise Admins”		✔	✔	Send-As	
“Enterprise Admins”		✔	✔	Receive-As	
“Domain Admins” of root domain		✔	✔	Send-As	
“Domain Admins” of root domain		✔	✔	Receive-As	
Everyone	✔		✔	ms-Exch-Create-Top-Level-Public-Folder	

				Public-Folder	
Everyone	✔		✔	ms-Exch-Create-Public-Folder	
Everyone	✔		✔	ms-Exch-Store-Create-Named-Properties	
Everyone	✔		✔	STANDARD_RIGHTS_READ | ACTRL_DS_READ_PROP | ACTRL_DS_LIST | ACTRL_LIST_OBJECT	Applies to object class: msExchPrivateMDB
Everyone	✔		✔	STANDARD_RIGHTS_READ | ACTRL_DS_READ_PROP | ACTRL_DS_LIST | ACTRL_LIST_OBJECT	Applies to object class: msExchPublicMDB
Everyone	✔		✔	STANDARD_RIGHTS_READ | ACTRL_DS_READ_PROP | ACTRL_DS_LIST | ACTRL_LIST_OBJECT	Applies to object class: mTA
Exchange Domain Servers	✔		✔	DS_AM_CONTROL_ACCESS (i.e, all extended rights)	
Exchange Domain Servers	✔		✔	ACTRL_DS_CREATE_CHILD	
Exchange Domain Servers	✔		✔	ACTRL_DS_WRITE_PROP	Public-Information (property set)
Exchange Domain Servers	✔		✔	ACTRL_DS_WRITE_PROP	Personal-Information (property set)
Exchange Domain Servers	✔		✔	DS_AM_FULL_CONTROL	Applies to object class: siteAddressing
When enabling an SRS (ACE is removed when SRS is disabled)					
MACHINE$	✔		✔	ACTRL_DS_LIST_OBJECT | ACTRL_DS_CREATE_CHILD| ACTRL_DS_DELETE_CHILD	

Address Lists container

cn=Address Lists Container,cn=<organization>,cn=Microsoft Exchange,cn=Services,cn=Configuration,dc=<domain>					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During Server install					
Authenticated Users	✔		✔	ACTRL_DS_LIST	

Addressing container

cn=Addressing,cn=<organization>,cn=Microsoft Exchange,cn=Services,cn=Configuration,dc=<domain>					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During Server install					
Authenticated Users	✔		✔	STANDARD_RIGHTS_READ | ACTRL_DS_READ_PROP | ACTRL_DS_LIST	

Recipient Update Services container

cn=Recipient Update Services,cn=Address Lists Container,cn=<organization>,cn=Microsoft Exchange,cn=…					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During Server install					
Exchange Domain Servers	✔		✔	DS_AM_FULL_CONTROL	

Administrative Group

cn=<admin group>,cn=Administrative Groups,cn=<organization>,cn=Microsoft Exchange,cn=…					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During Server install ***(set on attribute msExchPFDefaultAdminACL)***					
Authenticated Users	✔		✔	ms-Exch-Create-Public-Folder	

Default TLH

cn=Public Folders,cn=All Folder Hierarchies,cn=<admin group>,cn=Administrative Groups,cn=<organization>,cn=…					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During Server install ***(set on attribute msExchPFDefaultAdminACL)***					
Authenticated Users	✔		✔	ms-Exch-Create-Public-Folder	

CA container

cn=CA,cn=Advanced Security,cn=<admin group>,cn=Administrative Groups,cn=<organization>,cn=…					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During KMS install					
MACHINE$	✔		✔	DS_AM_FULL_CONTROL	
Authenticated Users	✔		✔	STANDARD_RIGHTS_READ | ACTRL_DS_READ_PROP	

Connections Container

cn=Connections,cn=<routing group>,cn=Routing Groups,cn=<admin group>,cn=Administrative Groups,cn=…					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During Server install					
Exchange Domain Servers	✔		✔	DS_AM_FULL_CONTROL	

Server object

cn=<server>,cn=Servers,cn=<admin group>,cn=Administrative Groups,cn=…					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During Server install, if the server is NOT a cluster VM					

MACHINE$	✔		✔	DS_AM_FULL_CONTROL	
During Server install, if the server IS a cluster VM					
Exchange Domain Servers	✔		✔	DS_AM_FULL_CONTROL	

Protocols Container

cn=Protocols,cn=<server>,cn=Servers,cn=<admin group>,cn=Administrative Groups,cn=…					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During Server install					
Everyone	✔		✔	ACTRL_DS_LIST	
Everyone	✔		✔	ms-Exch-Read-Metabase-Properties	

System Attendant object

cn=Microsoft System Attendant,cn=<server>,cn=Servers,cn=<admin group>,cn=Administrative Groups,cn=…					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During Server install ***(set on attribute msExchMailboxSecurityDescriptor)***					
LocalSystem	✔		✔	READ_CONTROL | fsdspermUserSendAs | fsdspermUserMailboxOwner	
Exchange Domain Servers	✔		✔	READ_CONTROL | fsdspermUserSendAs | fsdspermUserMailboxOwner	
5.5 Service Account (if given)	✔		✔	READ_CONTROL | fsdspermUserSendAs | fsdspermUserMailboxOwner	

MTA object

cn=Microsoft MTA,cn=<server>,cn=Servers,cn=<admin group>,cn=Administrative Groups,cn=…					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During Server install					
5.5 Service Account (if given)	✔		✔	Send-As	
5.5 Service Account (if given)	✔		✔	Read-As	

PERMISSIONS ON OTHER OBJECTS IN THE CONFIGURATION TREE:

Deleted Items container

cn=Deleted Items,cn=Configuration,dc=<domain>					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During ForestPrep phase					

Designated admin account	✔		✔	STANDARD_RIGHTS_READ | ACTRL_DS_LIST | ACTRL_DS_READ_PROP | ACTRL_DS_LIST_OBJECT | WRITE_OWNER | WRITE_DAC	
During Server install					
Exchange Domain Servers	✔		✔	ACTRL_DS_LIST	

Active Directory Connector object

cn=Active Directory Connector,cn=Exchange Settings,cn=<server>,cn=Servers,cn=<site>,cn=sites,cn=Configuration,…					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During ADC setup					
Exchange Services	✔		✔	DS_AM_FULL_CONTROL	
Authenticated Users	✔		✔	STANDARD_RIGHTS_READ | ACTRL_DS_READ_PROP | ACTRL_DS_LIST	

MachineEnrollmentAgent object

cn=MachineEnrollmentAgent,cn=Certificate Templates,cn=Public Key Services,cn=Services,cn=Configuration,cn=…					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During KMS install					
MACHINE$	✔		✔	DS_AM_FULL_CONTROL	

ExchangeUser object

cn=ExchangeUser,cn=Certificate Templates,cn=Public Key Services,cn=Services,cn=Configuration,cn=…					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During KMS install					
MACHINE$	✔		✔	READ_CONTROL | ACTRL_DS_LIST | ACTRL_DS_READ_PROP	
MACHINE$	✔		✔	Enroll	

ExchangeUserSignature object

cn=ExchangeUserSignature,cn=Certificate Templates,cn=Public Key Services,cn=Services,cn=Configuration,cn=…					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During KMS install					
MACHINE$	✔		✔	READ_CONTROL | ACTRL_DS_LIST | ACTRL_DS_READ_PROP	

MACHINE$	✔		✔	Enroll	

PERMISSIONS ON OBJECTS IN THE DOMAIN NAMING CONTEXT:

Domain container

dc=<domain>					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During DomainPrep phase					
Exchange Enterprise Servers	✔		✔	ACTRL_DS_WRITE_PROP	Public-Information (property set)
Exchange Enterprise Servers	✔		✔	ACTRL_DS_WRITE_PROP	Personal-Information (property set)
Exchange Enterprise Servers	✔		✔	ACTRL_DS_WRITE_PROP	groupType
Exchange Enterprise Servers	✔		✔	DS-Replication-Manage-Topology	

Domain proxy container

cn=Microsoft Exchange System Objects,dc=<domain>					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During DomainPrep phase					
Exchange Enterprise Servers	✔			DS_AM_FULL_CONTROL	
Exchange Domain Servers	✔		✔	DS_AM_FULL_CONTROL	

"Exchange Enterprise Servers" group

cn=Exchange Enterprise Servers,cn=Users,dc=<domain>					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During DomainPrep phase					
All org-level full Exchange admins	✔			DS_AM_FULL_CONTROL	
Exchange Enterprise Servers	✔			DS_AM_FULL_CONTROL	

"Exchange Domain Servers" group

cn=Exchange Domain Servers,cn=Users,dc=<domain>					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During DomainPrep phase					
All org-level full Exchange admins	✔			DS_AM_FULL_CONTROL	

Exchange Enterprise Servers	✔			DS_AM_FULL_CONTROL	